(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 694 034 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
23.08.2006 Bulletin 2006/34

(51) Int Cl.:
H04L 29/12 *(2006.01)*

(21) Application number: **05290348.1**

(22) Date of filing: **16.02.2005**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR LV MK YU

(71) Applicant: **ALCATEL**
75008 Paris (FR)

(72) Inventor: **Whal, Stefan**
71701 Schwieberdingen (DE)

(74) Representative: **Brose, Gerhard et al**
Alcatel,
Intellectual Property Department Stuttgart
70430 Stuttgart (DE)

(54) Method to establish a peer-to-peer connection between two user agents located behind symmetric NATs

(57) A method to establish an Internet connection between a first (1) and a second (2) user agent is described, wherein a NAT-table entry in a controllable NAT (7) located in the Internet (3) is generated, wherein said NAT-table entry comprises public IP-address:Port pairs that are communicated to the user agents (1, 2), wherein the user agents (1, 2) use said public IP-address:port pairs for establishing an Internet connection between each other via the controllable NAT (7).

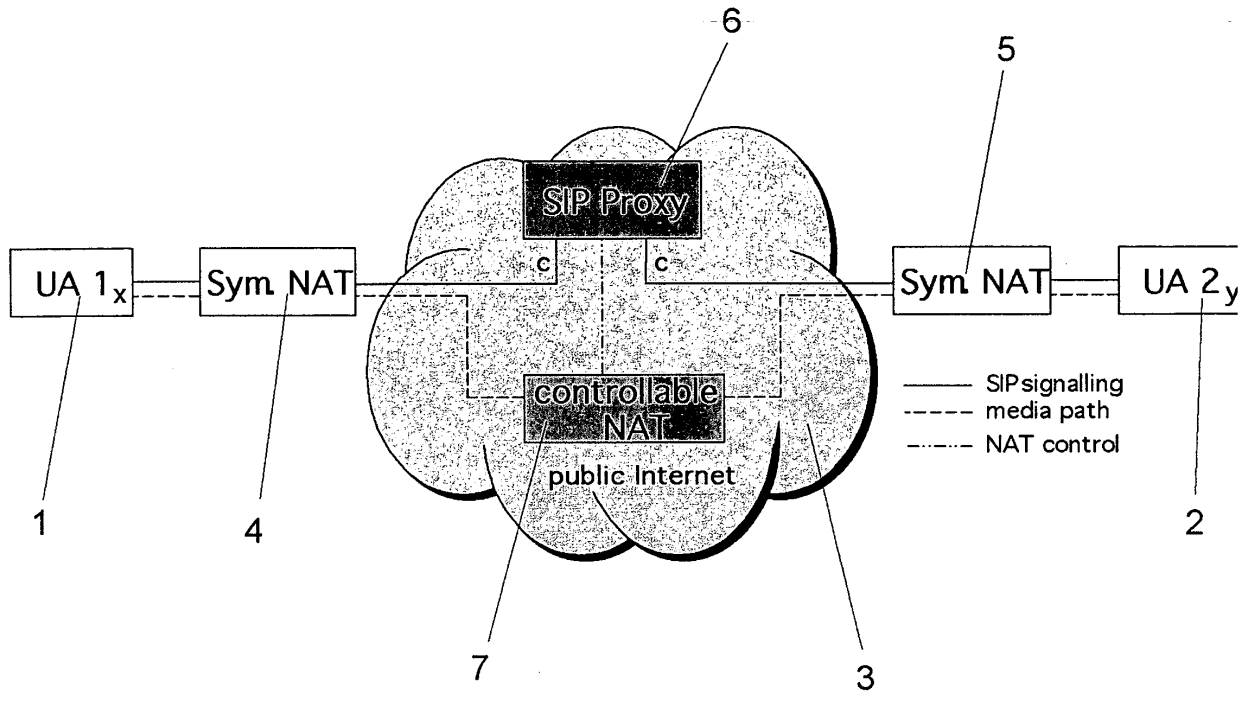

Fig. 1

EP 1 694 034 A1

Description

Technical field:

[0001] The invention relates to a method to establish an Internet connection between a first and a second user agent optionally each one located behind a symmetric NAT, according to the specifying features of claim 1.

Background of the invention:

[0002] Network Address Translation, NAT commonly is being used by many service providers and private individuals as a way to get around the problem of not having enough IP addresses. An enterprise may have a block of IP addresses assigned to them, but many more computers than the allocated IP addresses. Alternatively, an individual may have a DSL connection with one IP address, but want to have multiple computers hooked up to the Internet. NAT solves this problem by mapping internal addresses to external or public addresses. An internal IP-address:Port pair is mapped to an external IP-address:port pair, and whenever the NAT receives a packet with the external IP-address:Port pair, it knows how to reroute the packet back to the internal IP-address: Port pair.

[0003] There are four types of NATs known:

- full cone NAT
- restricted cone NAT
- port restricted cone NAT
- symmetric NAT.

[0004] A full cone NAT comprises a NAT table that stores temporary IP-address and port bindings. Each record in the NAT-table of a full cone NAT consists of the internal source IP-address of an internal device located on the private site of the NAT, the used internal source port and the assigned external source port on the Internet site of the NAT. Incoming packets from the Internet are allowed to get through the NAT if they are addressed to the external source port of the NAT. New entries within this NAT table are generated each time an outbound packet is sent to the public Internet. If incoming or outgoing packets do not refresh a NAT-table entry said entry will be withdrawn after a specified period of time. Thereby the full cone NAT accepts all incoming packets whose destination port matches an external source port comprised in any entry in the NAT table, independently from where the packet was sent.

[0005] In Fig. 3, showing an example of a full cone NAT, any public Internet host which addresses the NAT and uses the external source port 61795 of the NAT as destination port is accepted by the NAT and the NAT will translate the destination IP-address:port pair to 10.0.0.101:12836.

[0006] In contrast to the Full Cone NAT, a restricted cone NAT additionally uses a destination IP-address to identify inbound IP packets. Therefore, as shown in Fig. 4, the NAT table entry is extended by the public IP-address of a public Internet host. Restricted cone NATs use the external source IP-address and generate an external source port from the internal source IP-address and port, which means, that as long as those values do not change also the external source IP-address and port remains the same. If an application would use the same internal source port on the internal device to communicate with two different hosts on the public Internet, the external IP source port is exactly the same for both hosts, nevertheless two record entries are generated in the NAT table which differ only concerning the host IP addresses. However, the NAT will block packets coming from another host, until the client sends out a packet to said other hosts public IP-address. Once that is done, both hosts can send packets back to the same internal source port, and they will both have the same mapping through the NAT

[0007] The port restricted cone NAT is a further extension of the restricted cone NAT wherein the NAT will block all packets unless the internal device had previously sent out a packet to the IP-address and port of the host that is sending to the NAT. The port restricted cone NAT performs the follow check for every incoming packet: First, it extracts the destination port and verifies whether there exists an valid entry in the NAT table. If there is no entry then the packet is dropped. In the other case, the NAT compares the host IP-address:port pair with the NAT table entries. If these values match, the NAT performs the IP-address and port translations and forwards the packet to the internal device. Otherwise the packet is dropped (Fig. 5). The external source port used by the NAT is always the same as long as the internal source IP-address and port remain the same. The NAT table could store further entries that differ only concerning the destination IP-address:port pair.

[0008] The behaviour of the symmetric NAT is almost the same as for the port restricted cone NAT. The difference is that a specific mapping of internal source IP-address:port pair to the NAT's external source IP-address: port pair is dependant on the destination IP-address:port pair that the packet is sent to. As soon as one of these four values changes, the symmetric NAT generates at least a new external source port and adds a further entry in the NAT table (Fig. 6). Due to the strategy described above, the devices behind a symmetric NAT are very well secured against any kind of unfriendly access. But a drawback arises from the strong blocking situation in case of e.g. connection set-ups using e.g. the Session Initialization Protocol, SIP. Applications to be used e.g. to establish a peer-to-peer connection to be used for telephone communication via the Internet typically use SIP signaling. Such applications are known as user agents. The SIP signaling protocol has to tell the peer the destination IP-address:port pair for the upcoming media session during the set up phase. But the external port used by the symmetric NAT cannot be determined in advance and the symmetric NAT will generate a NAT port out of

the internal source IP-address:port pair of the device providing said user agent located behind the symmetric NAT and the destination IP-address:port pair at the very moment when the first packet is sent to the destination IP-address:port pair. If the other host is also shielded by a symmetric NAT, the worst case situation is reached.

[0009] To connect two user agents located behind symmetric NATs it is known to use relays located in the Internet. Such relays are adding a not negligible packet delay and are not scalable enough. Furthermore relays cut a peer-to-peer session into two sessions from relay to a first peer and from relay to a second peer. Moreover the relay involves functions above transport layer. Due to this, relays are not advantageous to be used e.g. to establish a connection between two user agents to be used for telephone calls via the Internet.

[0010] So up to now, no solution is known to peer-to-peer connect two user agents with each other when at least one is located behind a symmetric NAT.

[0011] Since today all kind of the described NATs are used, a potential solution should also be able to be used in combination with user agents not located behind NATs and also in combination with user agents located behind other NATs than symmetric NATs.

[0012] Such potential solutions are disclosed in the Internet Engineering Task Force Internet Draft "NAT and Firewall Scenarios and Solutions for SIP" , June, 2002. The problems of firewall and NAT traversal for SIP is classified as complex. This is due, in part, to the large number of different scenarios and the multitude of solutions developed to solve them. In this Internet Draft, various scenarios are enumerated which can arise, and for each, point to some of the existing solutions for that scenario are presented with call flows and explanations for how it works.

Technical purpose of the invention:

[0013] The technical purpose of the invention is to develop a method that allows establishing an Internet connection to be used to exchange data between two user agents, wherein at least one user agent can be located behind a symmetric NAT.

Disclosure of the invention and its advantages:

[0014] The invention's technical purpose is fully met by the proposed method to establish an Internet connection like e.g. a session between a first and a second user agent wherein a NAT-table entry in a controllable NAT located in the Internet is generated, e.g. by a server or by the controllable NAT itself, wherein said NAT-table entry comprises public IP-address:Port pairs that are communicated to the user agents e.g. by the server, wherein the user agents use said public IP-address:port pairs for establishing an Internet connection between each other via the controllable NAT.

[0015] Thereby it is important to mention that the public IP-address:port pairs are generated and entered into the NAT-table of the controllable NAT before a communication between the user agents takes place. Said public IP-address:port pairs are used as destination addresses to which the user agents send their data to be exchanged with each other. Since the public IP-address:port pairs belong to the controllable NAT, the communication between the user agents takes place via the controllable NAT by performing only NAT layer functions.

[0016] Said Method with the specifying features of claim 1 has the advantage over the state of the art, that it allows to establish a connection between two user agents that can be located behind symmetric NATs. Thereby the controllable NAT preferably is a symmetric NAT since this increases the security of the connection between the two user agents. The controllable NAT is a simple component that must not be SIP aware and that translates IP-addresses and port according to the entry in the NAT-table. The end-to-end packet delay only increases negligible. The invention allows to place multiple controllable NATs within the Internet so that the load can be distributed. Thereby, in a first embodiment, wherein a server generates the public IP-address:Port pairs to be entered into the NAT-table, it is possible that only few or only one server can control many controllable NATs located in the Internet. In a second embodiment, the controllable NAT itself generates the public IP-address:Port pairs to be entered into the NAT-table and offers these public IP-address:Port pairs to requesting servers. Furthermore controllable NAT functions can easily be added e.g. into routers. The Method allows to establish any connection between two user agents to be used to exchange data.

[0017] A preferred embodiment of the invention comprises the steps of:

- registration of both user agents at a server,
- sending an invitation message to establish a connection with the second user agent from the first user agent to the server, wherein said invitation message comprises a first destination IP-address:Port pair to which the second user agent shall reply,
- generation of a NAT-table entry in a controllable NAT located in the Internet by the server, wherein said NAT-table entry comprises a first and a second public IP-address:Port pair,
- replacing the first destination IP-address:Port pair within the invitation message with the first public IP-address:Port pair by the server and
- sending the changed invitation message comprising the first public IP-address:Port pair from the server to the second user agent,
- receiving the changed invitation message from the server by the second user agent and extracting the first public IP-address:Port pair out of said invitation message,
- sending a confirmation message to establish the connection with the first user agent from the second

user agent to the server, wherein said confirmation comprises a second destination IP-address:Port pair to which the first user agent shall reply,

- replacing the second destination IP-address:Port pair within the confirmation message with the second public IP-address:Port pair by the server and
- sending the changed confirmation message comprising the second public IP-address:Port pair from the server to the first user agent and
- receiving the changed confirmation message from the server by the first user agent and extracting the second public IP-address:Port pair out of said confirmation message,
- exchanging data between the first and the second user agent via the controllable NAT, wherein the first user agent addresses the data to be sent to the second user agent to the second public IP-address:Port pair extracted out of the confirmation message and wherein the second user agent addresses the data to be sent to the first user agent to the first public IP-address:Port pair extracted out of the invitation message, and
- completing the NAT-table entry of the controllable NAT by extracting a first source IP-address:Port pair from the very first data sent from the first user agent to the second user agent via the controllable NAT and a second source IP-address:Port pair from the very first data sent from the second user agent to the first user agent via the controllable NAT and inserting the first and the second source IP-address: Port pair into the NAT-table entry of the controllable NAT.

[0018] In a preferred embodiment of said invention, after receiving the confirmation message from the second user agent the server adds a first source IP-address of the first user agent comprised in the invitation message and a second source IP-address of the second user agent comprised in the confirmation message to the NAT-table entry of the controllable NAT, wherein the completion of the NAT-table entry is done by adding a first and a second source port of the first and the second user agent to the NAT-table entry comprised in the very first data exchange between the first and the second user agent via the controllable NAT.

[0019] In another preferred embodiment of said invention, at least one user agent is located behind a symmetric NAT.

[0020] In a preferred embodiment of said invention the server is a proxy server.

[0021] In a particular preferred embodiment of said invention the proxy server is a SIP proxy, wherein the invitation message and the confirmation message are SIP messages.

[0022] Another preferred embodiment of said invention the server is characterized in that the connection to be established between the user agents by the invitation and the confirmation message is a peer-to-peer connection.

[0023] In a preferred embodiment of said invention the data exchanged between the first and the second user agent comprise a media stream.

[0024] In a further preferred embodiment of said invention the media stream comprises a voice stream. The voice stream e.g. allows a first user using the first user agent to talk with a second user using the second user agent. By using the method according to the invention, telephone via Internet is possible for user agents located behind symmetric NATs.

[0025] A particular preferred embodiment of said invention is characterized in that at least one user agent is running on a computer. Preferably both user agents are running on computers. It is also thinkable, that one of the user agents is running on a Personal Digital Assistant, PDA or the like.

[0026] It is also thinkable that instead of the server the controllable NAT itself generates a new NAT-table entry comprising a first and a second public IP-address:Port pair, wherein the controllable NAT communicates said first and second public IP-address:Port pair to the server for replacing the first and the second destination IP-address:Port pair in the invitation message and in the confirmation message with the first and the second public IP-address:Port pair.

[0027] In another preferred embodiment of the invention, said method is performed by a computer program product stored on a computer usable medium comprising computer readable program means for causing a computer to perform the method mentioned above, when said computer program product is executed on a computer.

Brief description of the drawing, with

[0028]

Figure 1 showing a scheme of an arrangement to be used to execute the method according to the invention before a connection is established,
Figure 2 showing the arrangement of Fig. 1 after a connection has been established,
Figure 3 showing an example for a full cone NAT,
Figure 4 showing an example for a Restricted Cone NAT,
Figure 5 showing an example for a Port Restricted Cone NAT, and
Figure 6 showing an example for a symmetric NAT.

Paths for performing the invention:

[0029] As shown in Figure 1, a first 1 and a second user agent 2 are connected with the Internet 3. Both user agents 1, 2 are located behind symmetric NATs 4, 5. A proxy server 6 is located in the Internet 3. Also a controllable NAT 7 is located in the Internet. The controllable NAT 7 can be controlled by the proxy server 6, wherein the proxy server 6 is able to generate entries in the NAT-

table of the controllable NAT 7.

[0030] Figure 2 shows the situation when a peer-to-peer connection is established between the two user agents 1, 2 via the controllable NAT 7. The procedure to establish this connection is the following:

Both user agents 1 and 2 are registered at the proxy server 6. The first user agent 1 wants to establish a connection with the second user agent 2. To do this, an invitation message is sent from the first user agent 1 to the proxy server 6. This invitation message comprises a first destination IP-address:port pair to which the second user agent 2 shall reply. Since the first user agents 1 is located behind the symmetric NAT 4, a reply from the second user agent 2 to the first user agent 1 addressed to the first destination IP-address:port pair would be dropped at the symmetric NAT 4. To solve this problem, the proxy server 6 examines the invitation message and searches this first destination IP-address:port pair. The proxy server 6 replaces the first destination IP-address:port pair in the invitation message with a first public IP-address:port pair and forwards this changed invitation message to the second user agent 2 via the hole in the symmetric NAT 5 that has been generated with the registration of the second user agent 2 at the proxy server 6. At the same time the proxy server also generates a NAT-table entry in the controllable NAT 7. This NAT-table entry comprises the first public IP-address:port pair and a second public IP-address:port pair. The second user agent 2 receives the invitation message and extracts the first public IP-address:port pair out of said message. The second user agent 2 uses the first public IP-address:port pair to configure the destination address for all data packets, e.g. a data stream, sent to the first user agent 1. Then, the second user agent 2 generates a confirmation message and is sending this confirmation message to the proxy server 6. This confirmation message comprises a second destination IP-address:port pair to which the first user agent 1 shall reply. Since the second user agents 1 is located behind the symmetric NAT 5, a reply from the first user agent 1 to the second user agent 2 addressed to the second destination IP-address:port pair would be dropped at the symmetric NAT 5. To solve this problem, the proxy server 6 also replaces the second destination IP-address:port pair in the confirmation message with the second public IP-address:port pair and forwards this changed confirmation message to the first user agent 1 via the hole in the symmetric NAT 4 that has been generated with the registration of the first user agent 1 at the proxy server 6. The first user agent 1 receives the confirmation message and extracts the second public IP-address:port pair out of said message. The first user agent 1 uses the second public IP-address:port pair to configure the destination address for all data packets, e.g. a data stream, sent to the second user agent 2.

[0031] Now the first 1 and the second user agent 2 can communicate with each other via the controllable NAT. To complete the NAT-table entry in the controllable NAT 7, a first source IP-address:port pair is extracted from the very first data sent from the first user agent 1 to the second user agent 2 and a second source IP-address:port pair is extracted from the very first data sent from the second user agent 2 to the first user agent 1. The extraction of these source IP-address:port pairs is done by the controllable NAT. The first and the second source IP-address:port pair are inserted into the NAT-table entry of the controllable NAT. By doing so, the NAT-table entry of the controllable NAT considering the session between the first 1 and the second user agent 2 is completed.

[0032] It is important to mention that in Fig. 1 and 2 only a single controllable NAT 7 is shown to keep the figures concise, but the concept allows also arranging several controllable NATs in the Internet 3. In general the proxy server 6 is aware of several controllable NATs, so that it can distribute the load between different controllable NATs to prevent hot spots in the network as well as to rearrange media session paths through the Internet to overcome e.g. error situations, network quality of services degradations and the like. The concept is extendible towards a quality of services controlled load balancing system with data load accounting per media session.

[0033] In an alternative embodiment of the invention, the controllable NAT itself generates its NAT-table entries comprising public IP-address:port pairs. The controllable NAT communicates these public IP-address:port pairs to the proxy server. The proxy server uses these public IP-address:port pairs to replace the destination IP-address:port pairs in the invitation message and in the confirmation message. This embodiment differs from the example described above thereby, that instead of the proxy server the controllable NAT itself generates the NAT-table entry comprising public IP-address:port pairs. In order that the proxy server knows which public IP-address:port pairs can be used to replace the destination IP-address:port pairs in the invitation message and in the confirmation message, the public IP-address:port pairs comprised in the NAT-table entry generated by the controllable NAT are communicated from the controllable NAT to the proxy server.

Commercial applicability:

[0034] The invention is commercially applicable particularly in the field of production and operation of networks to be used for Internet traffic.

Claims

1. Method to establish an Internet connection between a first (1) and a second (2) user agent, **characterized**

in
that a NAT-table entry in a controllable NAT (7) located in the Internet (3) is generated, wherein said NAT-table entry comprises public IP-address:Port pairs that are communicated to the user agents (1, 2), wherein the user agents (1, 2) use said public IP-address:port pairs for establishing an Internet connection between each other via the controllable NAT (7).

2. Method according to claim 1, comprising the steps of

- registration of both user agents (1, 2) at a server (6),
- sending an invitation message to establish a connection with the second user agent (2) from the first user agent (1) to the server (6), wherein said invitation message comprises a first destination IP-address:Port pair,
- generation of a NAT-table entry in a controllable NAT (7) located in the Internet (3) by the server (6), wherein said NAT-table entry comprises a first and a second public IP-address: Port pair,
- replacing the first destination IP-address:Port pair within the invitation message with the first public IP-address:Port pair by the server (6) and
- sending the changed invitation message from the server (6) to the second user agent (2),
- receiving the changed invitation message by the second user agent (2) and extracting the first public IP-address:Port pair out of said invitation message,
- sending a confirmation message from the second user agent (2) to the server (6), wherein said confirmation comprises a second destination IP-address:Port pair,
- replacing the second destination IP-address: Port pair within the confirmation message with the second public IP-address:Port pair by the server (6) and
- sending the changed confirmation message comprising the second public IP-address:Port pair from the server (6) to the first user agent (1) and
- receiving the changed confirmation message by the first user agent (1) and extracting the second public IP-address:Port pair out of said confirmation message,
- exchanging data between the first (1) and the second user agent (2) via the controllable NAT (7), wherein the first user agent (1) addresses to the second public IP-address:Port pair and wherein the second user agent (2) addresses to the first public IP-address:Port pair, and
- completing the NAT-table entry of the controllable NAT (7) by extracting a first source IP-address:Port pair from the very first data sent from the first user agent (1) to the second user agent (2) via the controllable NAT (7) and a second source IP-address:Port pair from the very first data sent from the second user agent (2) to the first user agent (1) via the controllable NAT (7) and inserting the first and the second source IP-address:Port pair into the NAT-table entry of the controllable NAT (7).

3. Method according to claim 2,
characterized in
that the server (6) after receiving the confirmation message from the second user agent (2) adds a first source IP-address of the first user agent (1) comprised in the invitation message and a second source IP-address of the second user agent (2) comprised in the confirmation message to the NAT-table entry, and wherein the completion of the NAT-table entry is done by adding a first and a second source port of the first (1) and the second user agent (2) to the NAT-table entry comprised in the very first data exchange between the first (1) and the second user agent (2) via the configurable NAT (7).

4. Method according to claim 2 or 3,
characterized in
that at least one user agent (1, 2) is located behind a symmetric NAT (4, 5).

5. Method according to claim 2, 3 or 4,
characterized in
that the server is a proxy server (6).

6. Method according to claim 5,
characterized in
that the proxy server (6) is a SIP proxy, wherein the invitation message and the confirmation message are SIP messages.

7. Method according to one of the previous claims,
characterized in
that the connection is a peer-to-peer connection.

8. Method according to one of the previous claims,
characterized in
that the data exchanged between the first (1) and the second user agent (2) comprise a media stream.

9. Method according to claim 8,
characterized in
that the media stream comprises a voice stream.

10. Method according to one of the previous claims,
characterized in
that at least one user agent (1, 2) is running on a computer.

11. Method according to one of the claims 2 to 10,

characterized in
that instead of the server the controllable NAT itself generates a new NAT-table entry comprising a first and a second public IP-address:Port pair, wherein the controllable NAT communicates said first and second public IP-address:Port pair to the server for replacing the first and the second destination IP-address:Port pair in the invitation message and in the confirmation message with the first and the second public IP-address:Port pair.

12. Computer program product stored on a computer usable medium comprising computer readable program means for causing a computer to perform the method of anyone of the claims 1 to 11, when said computer program product is executed on a computer.

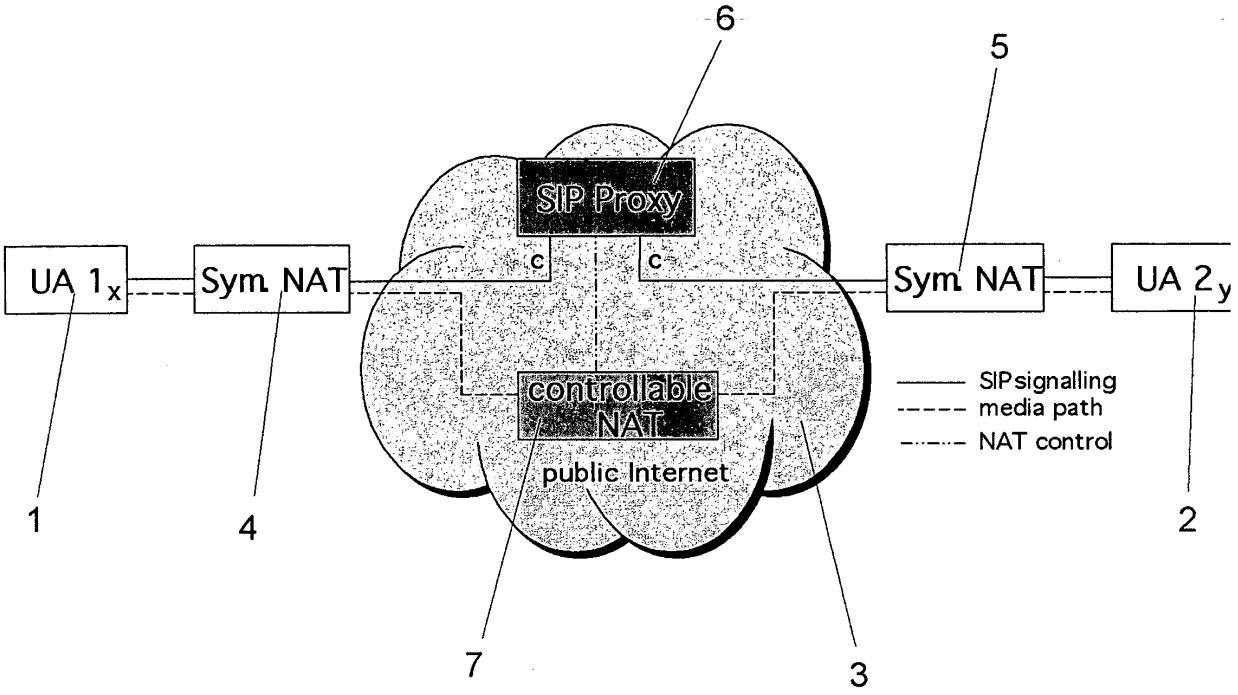
6
5
SIP Proxy
c
c
UA 1x
Sym. NAT
Sym. NAT
UA 2y
controllable NAT
public Internet
SIP signalling
media path
NAT control
1
4
7
3
2

Fig. 1

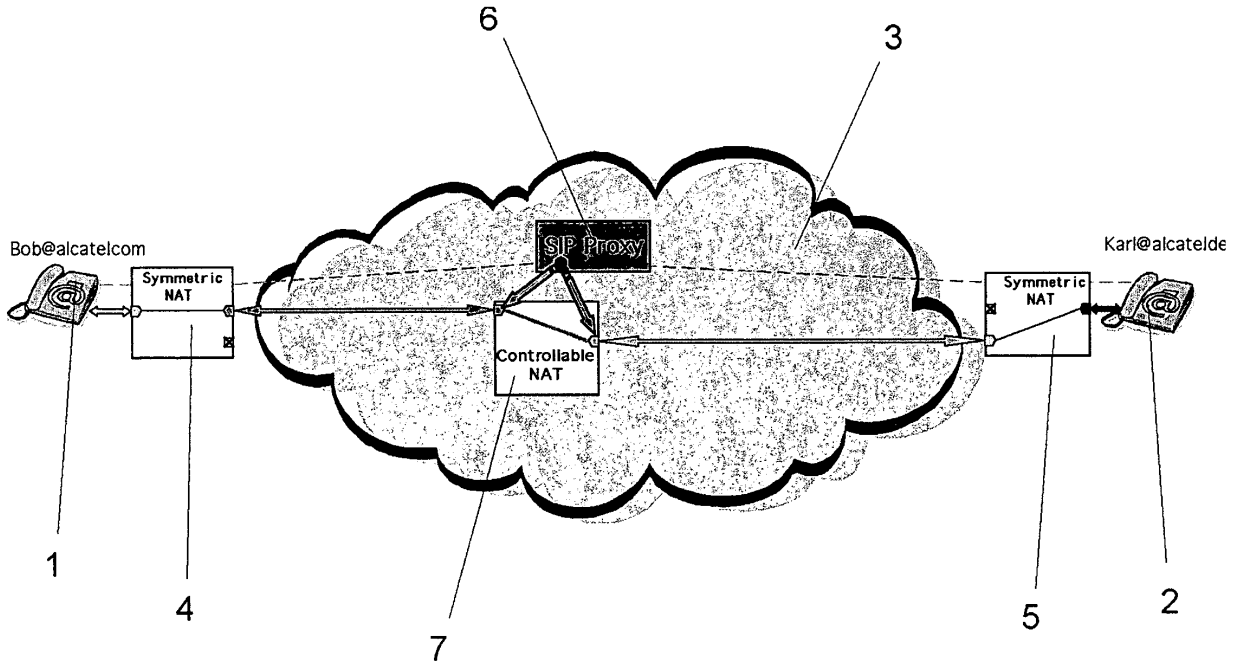
6
3
Bob@alcatelcom
SIP Proxy
Karl@alcatelde
Symmetric NAT
Symmetric NAT
Controllable NAT
1
4
7
5
2

Fig. 2

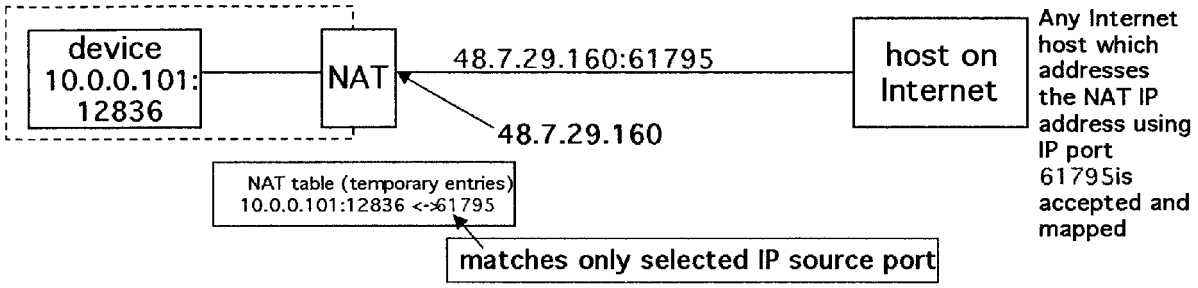
device
10.0.0.101:
12836
NAT
48.7.29.160:61795
48.7.29.160
host on
Internet
Any Internet
host which
addresses
the NAT IP
address using
IP port
61795is
accepted and
mapped
NAT table (temporary entries)
10.0.0.101:12836 <->61795
matches only selected IP source port

Fig. 3

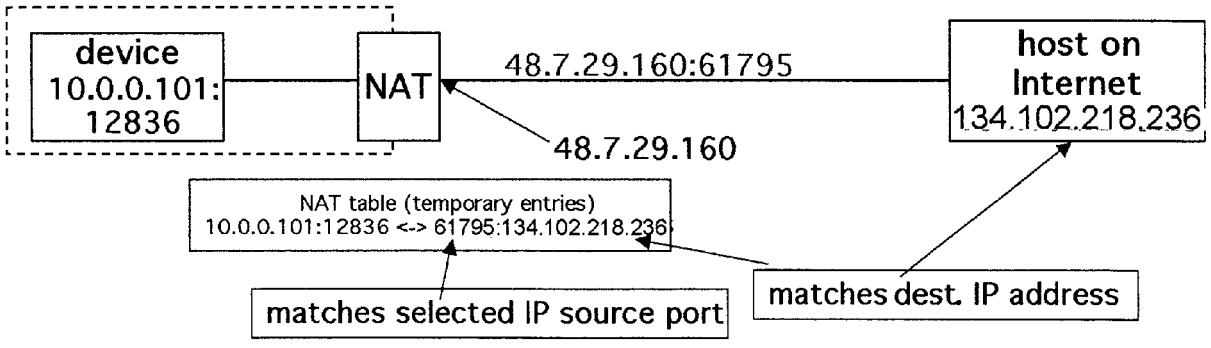
device
10.0.0.101:
12836
NAT
48.7.29.160:61795
48.7.29.160
host on
Internet
134.102.218.236
NAT table (temporary entries)
10.0.0.101:12836 <-> 61795:134.102.218.236
matches selected IP source port
matches dest. IP address

Fig. 4

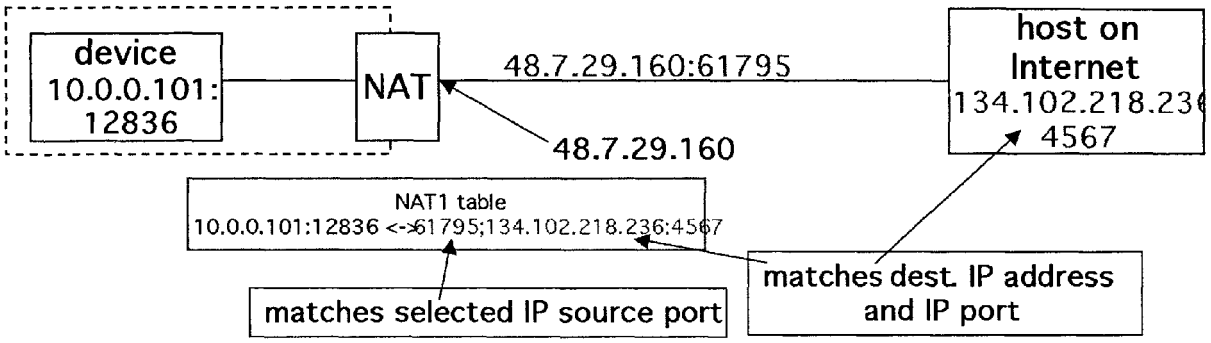
device
10.0.0.101:
12836
NAT
48.7.29.160:61795
48.7.29.160
host on
Internet
134.102.218.23
4567
NAT1 table
10.0.0.101:12836 <->61795;134.102.218.236:4567
matches selected IP source port
matches dest. IP address
and IP port

Fig. 5

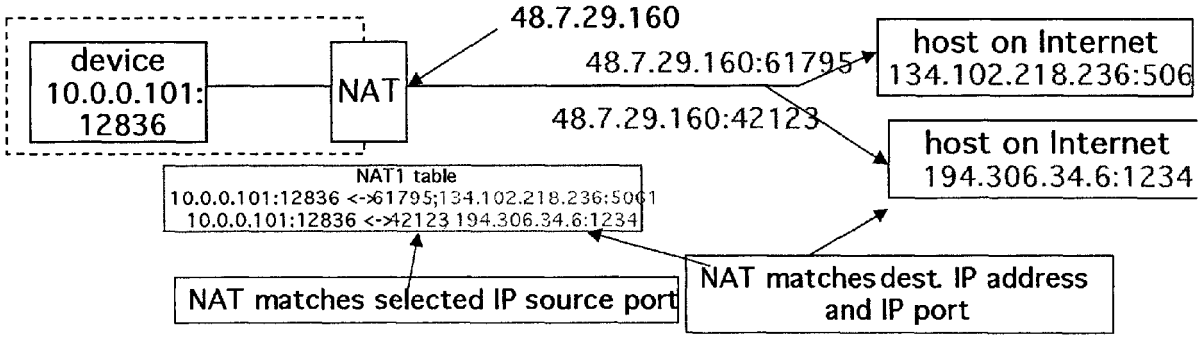
device
10.0.0.101:
12836
NAT
48.7.29.160
48.7.29.160:61795
48.7.29.160:42123
host on Internet
134.102.218.236:506
host on Internet
194.306.34.6:1234
NAT1 table
10.0.0.101:12836 <->61795;134.102.218.236:5061
10.0.0.101:12836 <->42123 194.306.34.6:1234
NAT matches selected IP source port
NAT matches dest. IP address
and IP port

Fig. 6

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 05 29 0348

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	J. ROSENBERG; R. MAHY; S. SEN: "NAT and Firewall Scenarios and Solutions for SIP" DRAFT-IETF-SIPPING-NAT-SCENARIOS-00.TXT, 24 June 2002 (2002-06-24), XP015003441 IETF, GENEVA	1,2, 4-10,12	H04L29/12
Y	Complete Chapter 5.2 "Solution II: External B2BUAWM" * page 46 - page 52 *	3,11	
X	EP 1 185 069 A (NORTEL NETWORKS LIMITED) 6 March 2002 (2002-03-06) * the whole document *	1,12	
Y	WO 2004/088923 A (TELEFONAKTIEBOLAGET LM ERICSSON ; LANDFELDT, BJOERN; SENEVIRATNE, ARUN) 14 October 2004 (2004-10-14) * page 13, line 1 - page 17, line 19 *	3	
A	STIEMERLING NEC H TSCHOFENIG SIEMENS M MARTIN NEC C AOUN NORTEL NETWORKS M: "NAT/Firewall NSIS Signaling Layer Protocol (NSLP)" IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, CH, vol. nsis, no. 1, 16 February 2004 (2004-02-16), XP015024465 ISSN: 0000-0004 * page 5 - page 10; figure 1 * Chapter 5.1 until (including) 5.3.4 * page 35 - page 39 *	3	TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04L
A	US 2004/177158 A1 (BAUCH DAVID JAMES ET AL) 9 September 2004 (2004-09-09) * paragraph '0110! - paragraph '0118!; figures 11-13 *	3	

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	28 July 2005	Raible, M

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 05 29 0348

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
Y	US 2002/085561 A1 (CHOI JEONG-HYUN ET AL) 4 July 2002 (2002-07-04) * paragraph '0031!; figures 6,7,8a * * paragraph '0050! - paragraph '0069! *	11	
A	US 2003/118002 A1 (BRADD PATRICK ET AL) 26 June 2003 (2003-06-26) * paragraph '0040! - paragraph '0049!; figures 4,5 *	11	
			TECHNICAL FIELDS SEARCHED (Int.Cl.7)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	28 July 2005	Raible, M

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

Application Number
EP 05 29 0348

CLAIMS INCURRING FEES

The present European patent application comprised at the time of filing more than ten claims.

☐ Only part of the claims have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims and for those claims for which claims fees have been paid, namely claim(s):

☐ No claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims.

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

see sheet B

☒ All further search fees have been paid within the fixed time limit. The present European search report has been drawn up for all claims.

☐ As all searchable claims could be searched without effort justifying an additional fee, the Search Division did not invite payment of any additional fee.

☐ Only part of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the inventions in respect of which search fees have been paid, namely claims:

☐ None of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims, namely claims:

European Patent Office

LACK OF UNITY OF INVENTION
SHEET B

Application Number
EP 05 29 0348

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1. claims: 1,2,4-10,12

   A system for call setup between users located behind symmetric NATs, whereby server configures address/port pairs in NAT device.

   ---

2. claim: 3

   An alternative configuration for server controlled entries in a NAT device and alternative completion procedure for NAT table entries.

   ---

3. claim: 11

   An alternative generation procedure for entries in a NAT device, i.e. values are chosen by NAT device itself.

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 05 29 0348

This annex lists the patent family membersrelating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

28-07-2005

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1185069 A	06-03-2002	CA 2352911 A1	28-02-2002
		EP 1185069 A2	06-03-2002
WO 2004088923 A	14-10-2004	AU 2003251265 A1	25-10-2004
		WO 2004088923 A1	14-10-2004
US 2004177158 A1	09-09-2004	US 2004177359 A1	09-09-2004
		WO 2004081715 A2	23-09-2004
		WO 2004082152 A2	23-09-2004
US 2002085561 A1	04-07-2002	KR 2002057079 A	11-07-2002
US 2003118002 A1	26-06-2003	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82